IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for determining whether a sender seeking to send a message to a receiving computer system via a network is an authorized sender, comprising:

receiving from the sender a request to communicate;

selecting a number N1;

calculating a hash value for the number N1 using a predetermined cryptographic hash function; ~~and~~

sending the hash value to the sender[[.]];

receiving from the sender a second number N2;

calculating a hash value for the number N2 using the predetermined cryptographic hash function;

comparing the hash value for the number N1 with the hash value for the number N2; and

processing a message received from the sender if at least a prescribed nonzero number of bits of the hash value for the number N1 match the corresponding bits of the hash value for the number N2;

wherein the number N2 is determined by an authorized sender by using the predetermined cryptographic hash function to search for a number (N2) such that at least the prescribed nonzero number of bits of the hash value for the number N2 match the corresponding bits of the hash value for the number N1.

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Canceled)

6. (Currently amended) The method of claim [[5]] 1, wherein the hash values are each Y bits long and the requirement that at least a prescribed nonzero number of bits of the hash value

for the number N1 match the corresponding bits of the hash value for the number N2 is considered to be satisfied ~~the hash value for number N1 matches the hash value for the number N2 sufficiently~~ if the first X bits of the hash value for number N1 are the same as the first X bits of the hash value for number N2.

7. (Currently amended) The method of claim [[4]] 1, further comprising not processing a message from the sender if ~~the hash value for the number N1 does not match the hash value for the number N2 sufficiently.~~ it is not the case that at least a prescribed nonzero number of bits of the hash value for the number N1 match the corresponding bits of the hash value for the number N2.

8. (Original) The method of claim 1, wherein the number N1 is a random number.

9. (Original) The method of claim 1, wherein the number N1 is a random number generated by a pseudo random number generator.

10. (Canceled)

11. (Currently amended) The method of claim 1[[0]], wherein the cryptographic hash function is the Secure Hash Algorithm (SHA-1).

12. (Currently amended) The method of claim 1, further comprising the sender finding [[a]] the second number N2.

13. (Currently amended) A method for determining whether a sender seeking to send a message to a receiving computer system via a network is an authorized sender, comprising:

receiving from the sender a request to communicate, the request to communicate comprising a number N and a timestamp T;

calculating a hash value for the number N and a hash value for the timestamp T using a predetermined cryptographic hash function; and

determining whether at least a prescribed nonzero number of bits of the hash value for the number N matche~~s~~ the corresponding bits of the hash value for the timestamp T ~~sufficiently~~[[.]];

wherein the number N is determined by an authorized sender by using the predetermined cryptographic hash function to search for a number (N) such that at least a prescribed nonzero number of bits of the hash value for the number N match the corresponding bits of the hash value for the timestamp T.

14. (Currently amended) The method of claim 13, further comprising processing a message received from the sender if at least a prescribed nonzero number of bits of the hash

value for the number N matches the corresponding bits of the hash value for the timestamp T ~~sufficiently~~.

15. (Original) The method of claim 13, further comprising determining whether the number N has been used in any prior request to communicate.

16. (Original) The method of claim 15, further comprising ignoring a message received from the sender if the number N has been used in any prior request to communicate.

17. (Original) The method of claim 13, further comprising determining whether the timestamp T is within a prescribed interval of the current time.

18. (Original) The method of claim 13, further comprising ignoring a message received from the sender if the timestamp T is not within a prescribed interval of the current time.

19. (Currently amended) A system for determining whether a sender seeking to send a message to a receiving computer system via a network is an authorized sender, comprising:

a computer associated with the network configured to: ~~receive from the sender a request to communicate, select a number N1, calculate a hash value for the number N1, and send the hash value to the sender.~~

receive from the sender a request to communicate;

select a number N1;

calculate a hash value for the number N1 using a predetermined cryptographic hash function;

send the hash value calculated for the number N1 to the sender;

receive from the sender a second number N2;

calculate a hash value for the number N2 using the predetermined cryptographic hash function;

compare the hash value for the number N1 with the hash value for the number N2; and

process a message received from the sender if at least a prescribed nonzero number of bits of the hash value for the number N1 match the corresponding bits of the hash value for the number N2;

wherein the number N2 is determined by an authorized sender by using the predetermined cryptographic hash function to search for a number (N2) such that at least the prescribed nonzero number of bits of the hash value for the number N2 match the corresponding bits of the hash value for the number N1.

20. (Currently amended) A computer program product for determining whether a sender seeking to send a message to a receiving computer system via a network is an authorized sender, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

receiving from the sender a request to communicate;

selecting a number N1;

calculating a hash value for the number N1 using a predetermined cryptographic hash function; ~~and~~

sending the hash value to the sender[[.]];

receiving from the sender a second number N2;

calculating a hash value for the number N2 using the predetermined cryptographic hash function;

comparing the hash value for the number N1 with the hash value for the number N2; and

processing a message received from the sender if at least a prescribed nonzero number of bits of the hash value for the number N1 match the corresponding bits of the hash value for the number N2;

wherein the number N2 is determined by an authorized sender by using the predetermined cryptographic hash function to search for a number (N2) such that at least the prescribed nonzero number of bits of the hash value for the number N2 match the corresponding bits of the hash value for the number N1.